ENTERPRISE CYBER DEFENSE

AutoSOC

Modern Hybrid Network Infrastructure

Integrating Ansible, Wazuh, Tines SOAR, and Groq LLM for Automated Multi-Site Enterprise Network Threat Response

PREPARED BY

Marwa Saaadallah Alknany

SUPERVISED BY

Dr/Ahmed Zakzouk

INSTITUTION

Al-Azhar university
communication and electronics Engineering

DATE

6/7/2026

Presentation Agenda

01 Problem Statement

02 Project Objectives

03 System Architecture

04 Network Topology

05 Tools & Technologies

06 Layer A — Infrastructure

07 Layer B — Automation (Ansible)

08 Layer C — AI-Driven SOC

09 Testing & Results

10 Conclusion & Future Work

Problem Statement

Manual Configuration

Configuring routers & firewalls command-by-command is time-consuming, inconsistent, and highly error-prone at scale.

Reactive Security

Traditional SIEMs generate thousands of raw alerts daily without context or remediation — leading to Alert Fatigue.

AI Privacy Risks

Sending sensitive logs to cloud AI exposes internal IP schemas, credentials, and security data to external servers.

Project Objectives

Design & Simulate

Architect a secure, multi-site enterprise network with real Cisco IOL devices inside PNetLab.

Automate with IaC

Deploy the entire network configuration from a single Ansible command — zero manual CLI interaction.

Build an AI-Driven SOC

Wazuh + Tines + VirusTotal + Groq AI — real-time detection, enrichment, and intelligent analysis.

Instant Notifications

Deliver AI-generated threat reports to the analyst via Telegram and Gmail within seconds of detection.

Three-Layer Architecture

Layer A

Infrastructure

Cisco IOL · pfSense · OSPF · IPsec VPN

Layer B

Automation

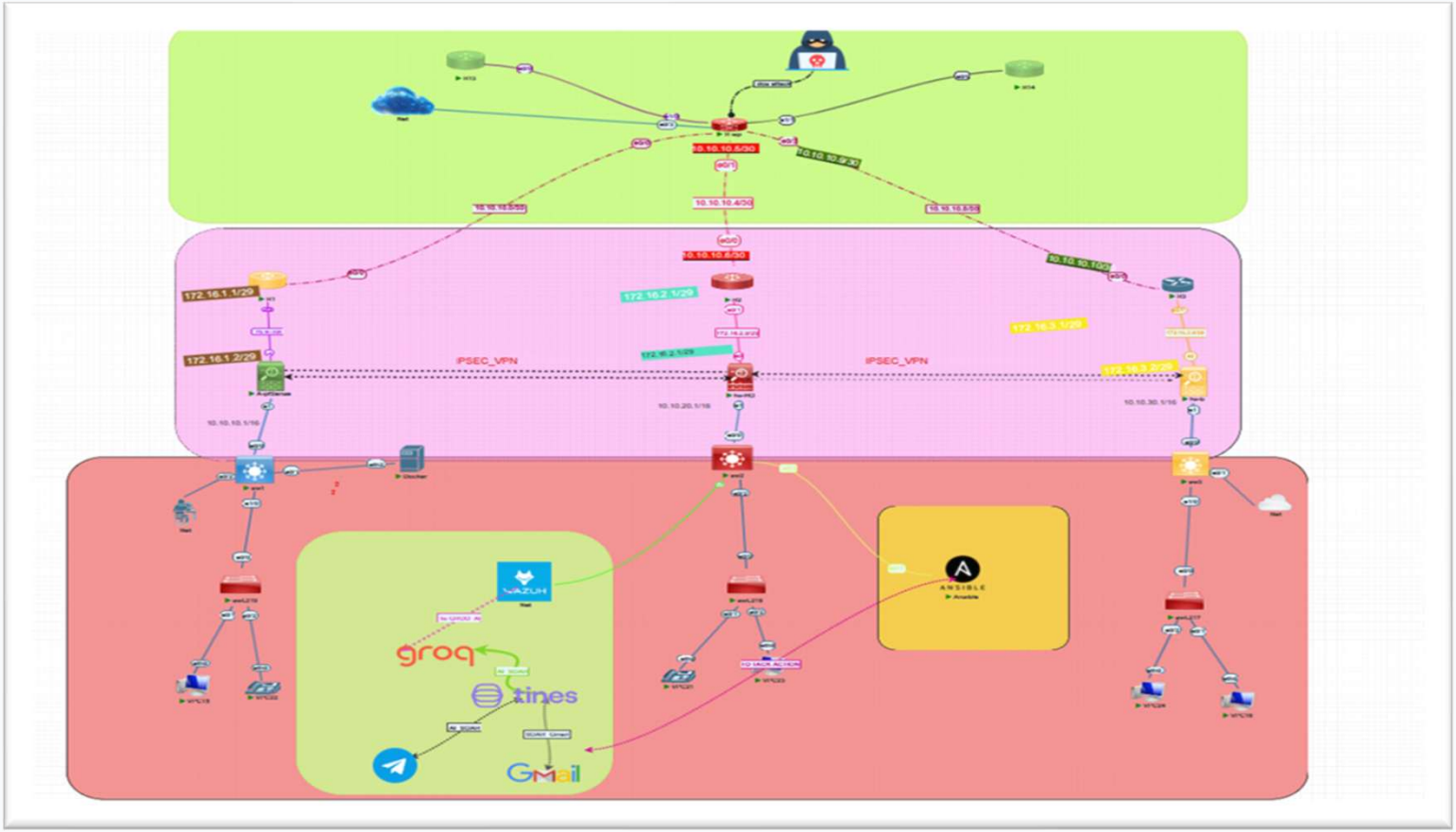
Ansible · Infrastructure as Code

Layer C

Intelligence

Wazuh · Tines · VirusTotal · Groq AI

Network Topology — Three-Site Enterprise



Branch A · 172.16.1.x / 10.10.10.0/30

HQ · 172.16.2.x / 10.10.10.4/30

Branch B · 172.16.3.x / 10.10.10.8/30

Tools & Technologies

PNetLab

Network simulation (Cisco IOL)

pfSense CE

Firewall + VPN + DHCP × 3 sites

Ansible

Infrastructure as Code automation

Wazuh XDR

SIEM — log collection & detection

Tines SOAR

No-code workflow orchestration

VirusTotal

Threat intelligence & IP reputation

Groq AI

LLM — threat analysis (Llama3)

Telegram

Real-time alert notifications

LAYER A

Infrastructure Layer — Secure Connectivity

Cisco IOL Routers

4 routers (ISP, HQ-R, BR-A, BR-B) running Cisco IOS 15.7 — authentic routing behavior without physical hardware.

pfSense Firewall × 3

Stateful inspection, default-deny rules, DHCP server, and IPsec VPN termination at every site boundary.

OSPF Dynamic Routing

FULL/DR adjacencies confirmed across all sites. Routes propagate automatically — no static route management.

IPsec Site-to-Site VPN

AES-256 encrypted tunnels between all three pfSense firewalls — all inter-site traffic is cryptographically protected.

LAYER B

Automation Layer — Infrastructure as Code

```
$ ansible-playbook site.yml
```

One command deploys the entire network across all three sites

playbook_network.yml

IP addresses + interfaces + hostnames

playbook_ospf.yml

OSPF areas + neighbor config

playbook_logging.yml

Syslog to Wazuh on all routers

playbook_wazuh.yml

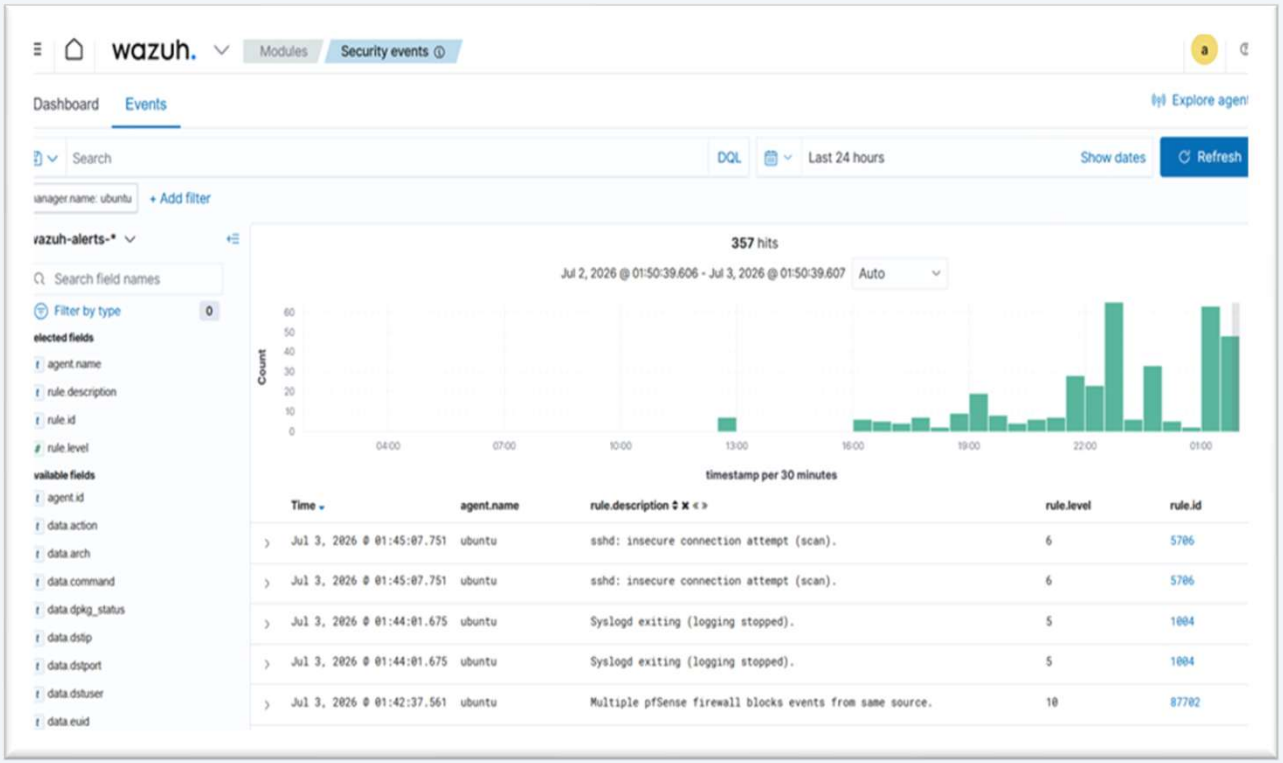
Agent install on all Linux hosts

LAYER C

Intelligence Layer — AI-Driven SOC

LAYER C

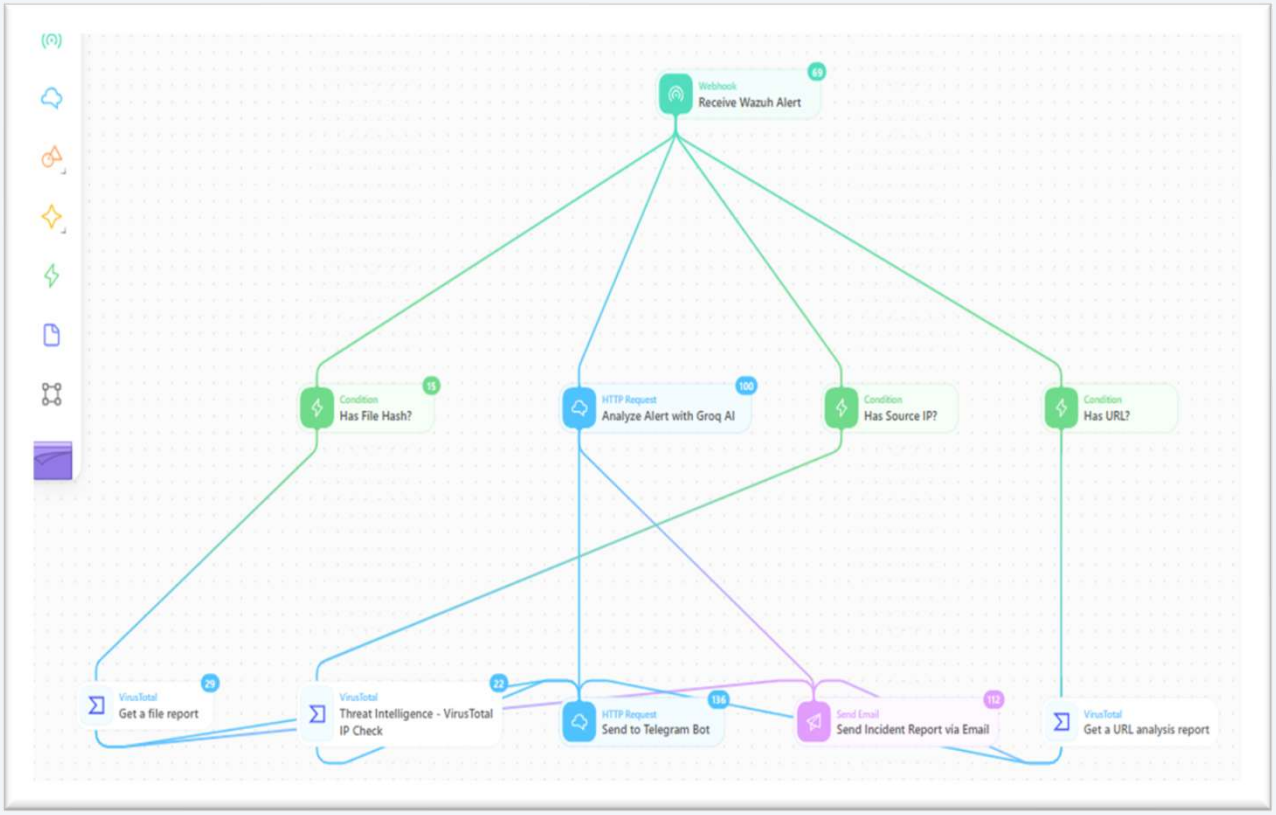
Wazuh XDR — Detection & Monitoring



- Manager-Agent architecture
- Real-time dashboard with forensic drill-down
- Active response triggers Tines webhook
- Collects syslog from all Cisco devices

LAYER C

Tines SOAR — Automated Response Workflow



1. Receives alert via Wazuh webhook
2. Queries VirusTotal for IP reputation
3. Sends enriched data to Groq AI
4. Delivers report to Telegram & Gmail

LAYER C

VirusTotal — Threat Intelligence Enrichment

```
// VirusTotal API Response
{
  "data": {
    "attributes": {
      "last_analysis_stats": {
        "malicious": 2,
        "suspicious": 0,
        "harmless": 0,
        "undetected": 69
      },
      "reputation": -6
    }
  }
```

2	-6	Potentially Malicious
Malicious Detections	Reputation Score	Verdict

LAYER C

Groq AI — Intelligent Threat Analysis

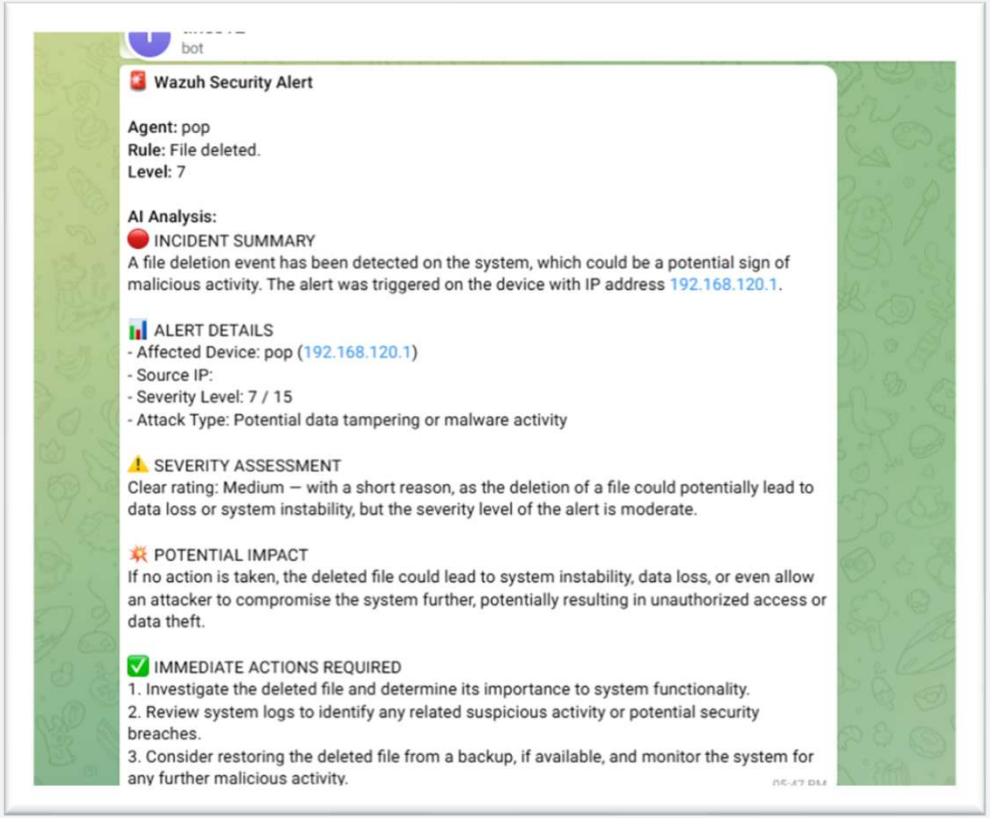

```
{
"incident_type": "File Integrity Modification",
"severity": "High",
"severity_level": 7,
"affected_host": "pop",
"affected_ip": "192.168.120.1",
"target_file": "C:\\Users\\marwa\\Downloads\\freevideo.exe",
"mitre": {
"id": "T1565.001",
"technique": "Stored Data Manipulation"
},

"analysis": "Wazuh File Integrity Monitoring detected that the monitored executable was modified.
The integrity checksum changed, indicating the file was altered after creation. The modification
should be validated to determine whether it is authorized or malicious.",

"recommended_actions": [
"Verify the file modification.",
"Compare the SHA256 hash with a trusted baseline.",
"Analyze the file using VirusTotal or a sandbox.",
```

LAYER C

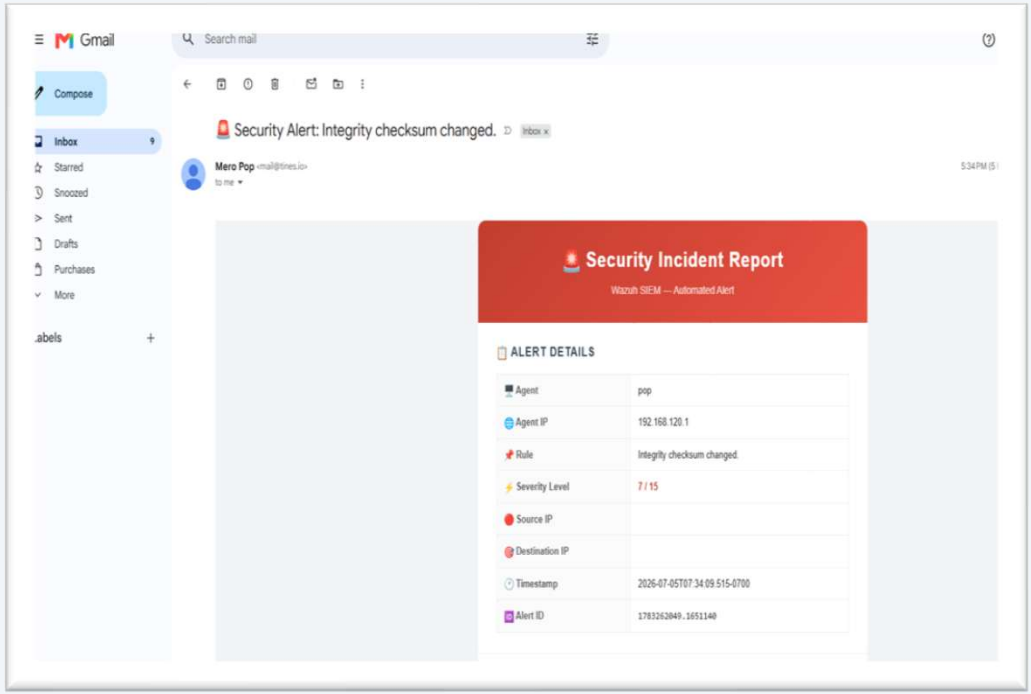
Telegram — Real-Time Alert Delivery


bot
Wazuh Security Alert
Agent: pop
Rule: File deleted.
Level: 7
AI Analysis:
INCIDENT SUMMARY
A file deletion event has been detected on the system, which could be a potential sign of malicious activity. The alert was triggered on the device with IP address 192.168.120.1.
ALERT DETAILS
- Affected Device: pop (192.168.120.1)
- Source IP:
- Severity Level: 7 / 15
- Attack Type: Potential data tampering or malware activity
SEVERITY ASSESSMENT
Clear rating: Medium — with a short reason, as the deletion of a file could potentially lead to data loss or system instability, but the severity level of the alert is moderate.
POTENTIAL IMPACT
If no action is taken, the deleted file could lead to system instability, data loss, or even allow an attacker to compromise the system further, potentially resulting in unauthorized access or data theft.
IMMEDIATE ACTIONS REQUIRED
1. Investigate the deleted file and determine its importance to system functionality.
2. Review system logs to identify any related suspicious activity or potential security breaches.
3. Consider restoring the deleted file from a backup, if available, and monitor the system for any further malicious activity.

- Delivered within seconds of attack detection
- Contains full AI-generated analysis and commands
- Accessible from any device — no VPN required
- Zero cost — Telegram Bot API is free

LAYER C

Email — Real-Time Alert Delivery



- Delivered within seconds of attack detection
- Contains full AI-generated analysis and commands
- Accessible from any device — no VPN required
- Zero cost — Telegram Bot API is free

Attack Simulation

Scenario 1 — SSH Brute Force

```
hydra -l root -P rockyou.txt ssh://10.10.20.x -t 4 -V
```

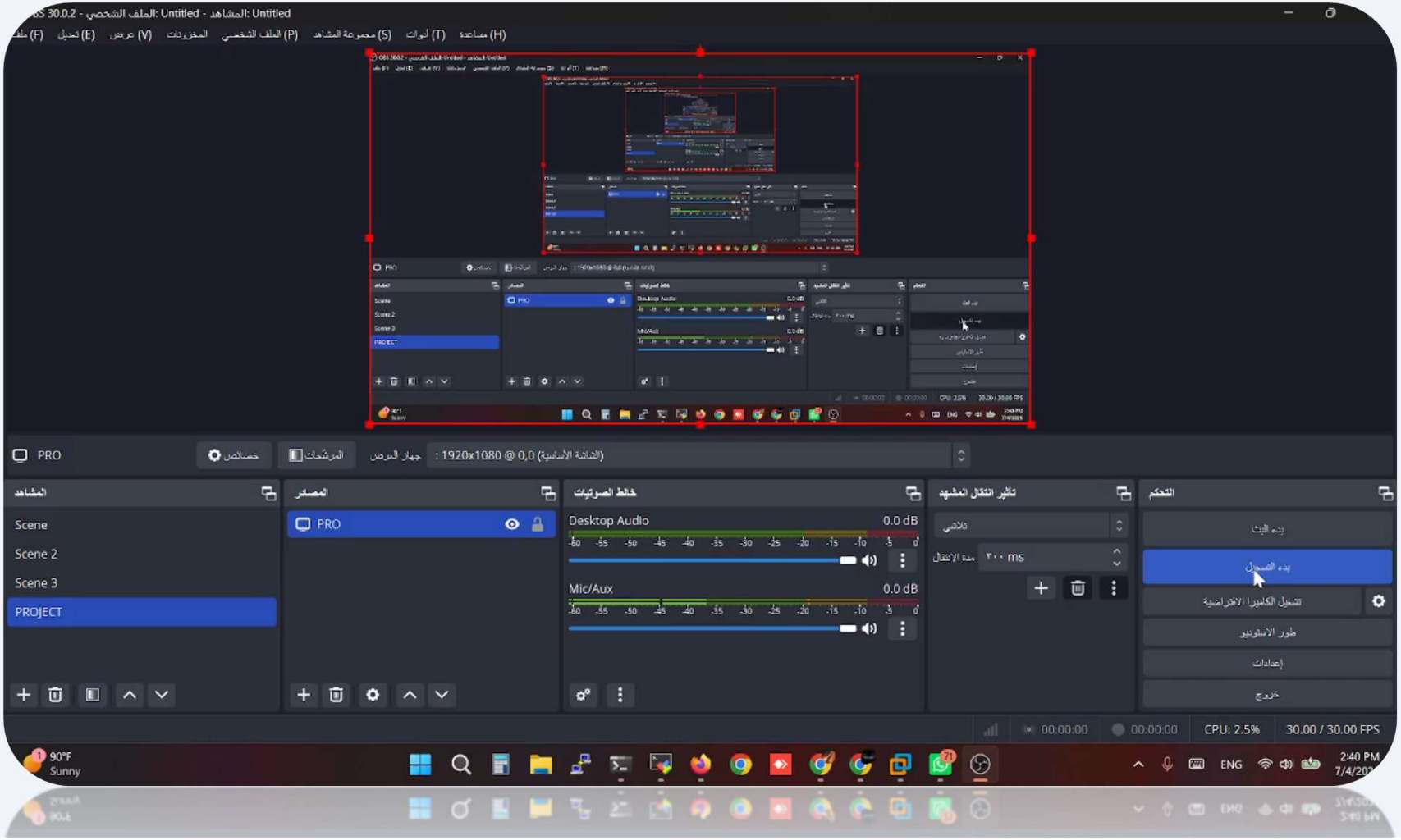
Hydra iterates a password dictionary against SSH — generates high-volume failed auth events detected by Wazuh Rule 5763.

Scenario 2 — Network Reconnaissance

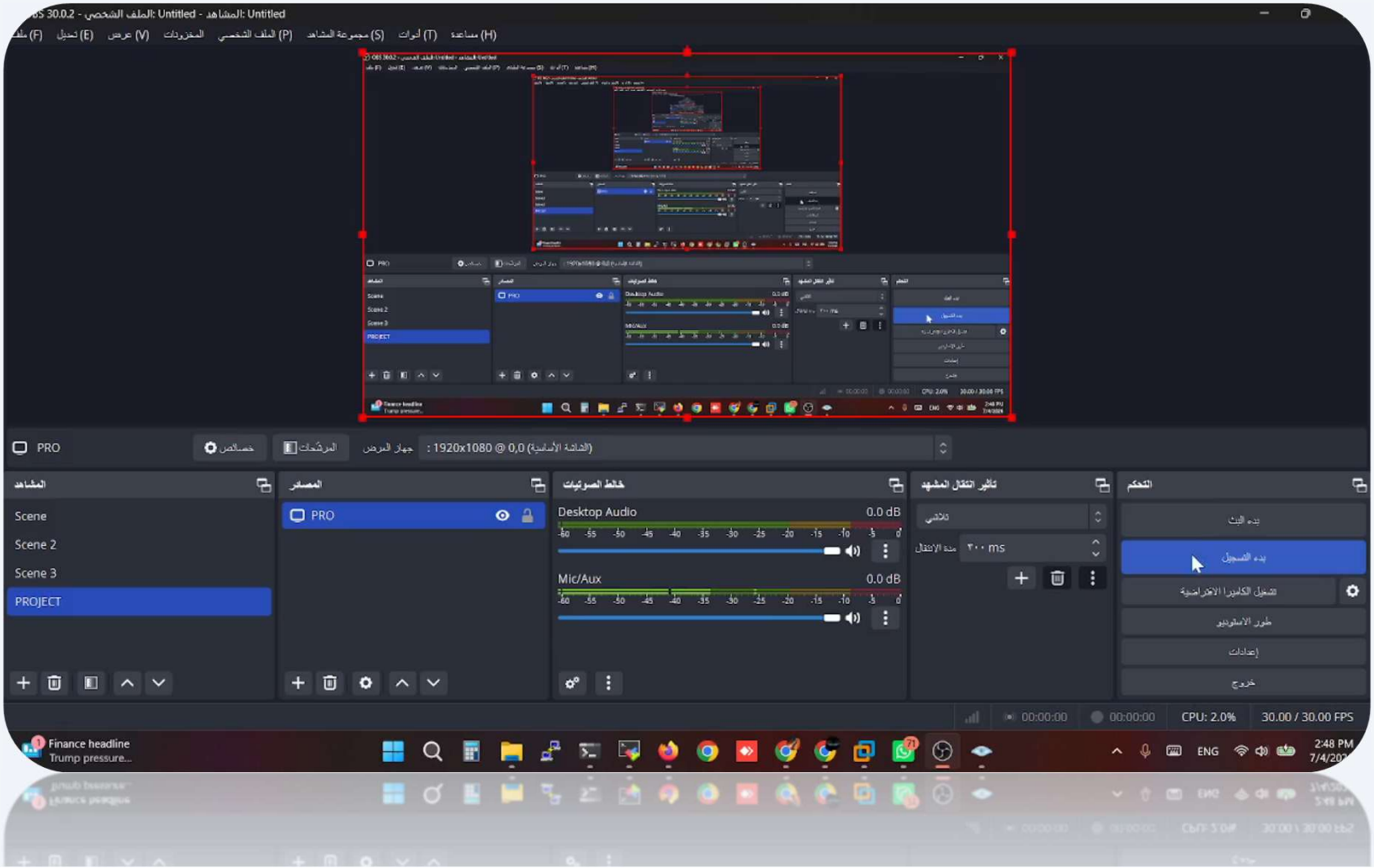
```
nmap -sV -A -T4 10.10.20.0/24
```

Aggressive port scan with service detection — triggers Wazuh reconnaissance detection rules across the HQ subnet.

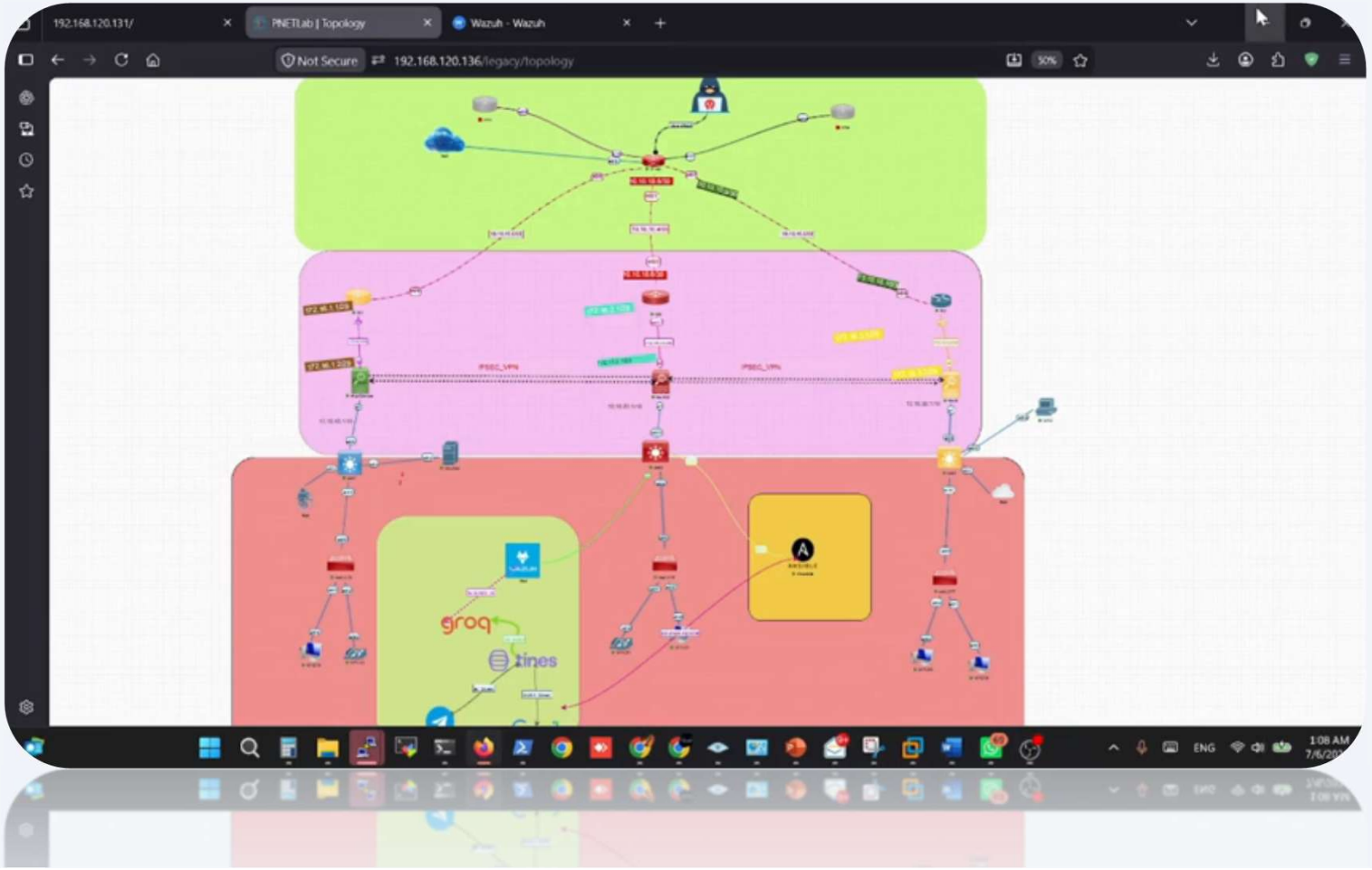
Testing Results Summary



Testing Results Summary



Testing Results Summary



Conclusion & Future Work

Achievements

- Multi-site enterprise network — fully automated
- Zero manual CLI interaction — all via Ansible
- Real-time AI threat analysis in under 3 seconds
- Complete detection-to-notification pipeline verified

Future Work

- SDN integration (OpenDaylight controller)
- Suricata IPS on pfSense for deep inspection
- Local LLM deployment (Ollama) for air-gap AI
- AWS/Azure hybrid cloud VPN extension

Thank You

Modern Hybrid Network Infrastructure · Graduation Project 2025/2026

ENTERPRISE CYBER DEFENSE

AutoSOC

Modern Hybrid Network Infrastructure

Integrating Ansible, Wazuh, Tines SOAR, and Groq LLM for Automated Multi-Site Enterprise Network Threat Response

PREPARED BY

Marwa Saaadallah Alknany

SUPERVISED BY

Dr/Ahmed Zakzouk

INSTITUTION

Al-Azhar university
communication and electronics Engineering

DATE

6/7/2026

Presentation Agenda

01 Problem Statement

02 Project Objectives

03 System Architecture

04 Network Topology

05 Tools & Technologies

06 Layer A — Infrastructure

07 Layer B — Automation (Ansible)

08 Layer C — AI-Driven SOC

09 Testing & Results

10 Conclusion & Future Work

Problem Statement

Manual Configuration

Configuring routers & firewalls command-by-command is time-consuming, inconsistent, and highly error-prone at scale.

Reactive Security

Traditional SIEMs generate thousands of raw alerts daily without context or remediation — leading to Alert Fatigue.

AI Privacy Risks

Sending sensitive logs to cloud AI exposes internal IP schemas, credentials, and security data to external servers.

Project Objectives

Design & Simulate

Architect a secure, multi-site enterprise network with real Cisco IOL devices inside PNetLab.

Automate with IaC

Deploy the entire network configuration from a single Ansible command — zero manual CLI interaction.

Build an AI-Driven SOC

Wazuh + Tines + VirusTotal + Groq AI — real-time detection, enrichment, and intelligent analysis.

Instant Notifications

Deliver AI-generated threat reports to the analyst via Telegram and Gmail within seconds of detection.

Three-Layer Architecture

Layer A

Infrastructure

Cisco IOL · pfSense · OSPF · IPsec VPN

Layer B

Automation

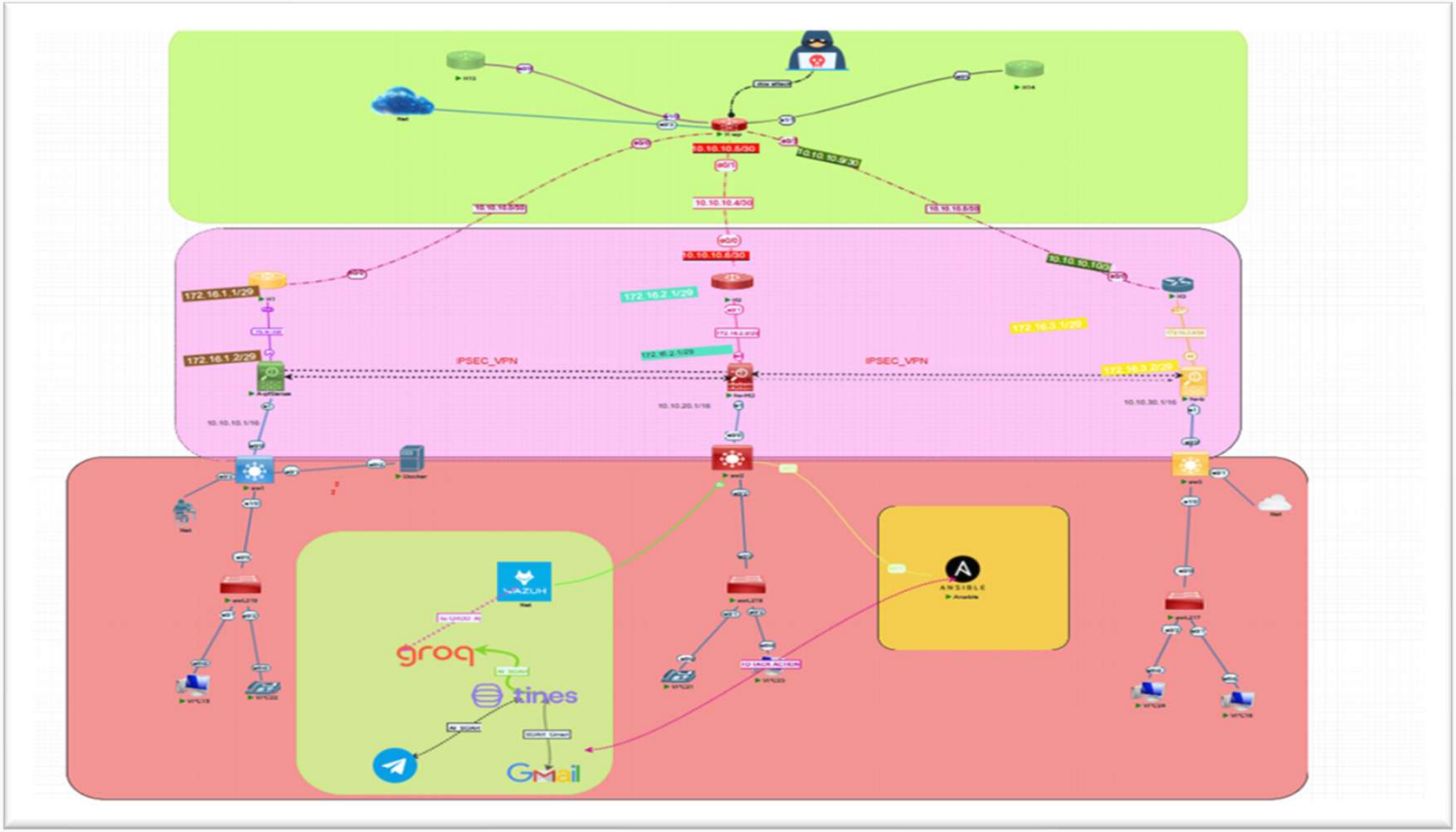
Ansible · Infrastructure as Code

Layer C

Intelligence

Wazuh · Tines · VirusTotal · Groq AI

Network Topology — Three-Site Enterprise



Branch A · 172.16.1.x / 10.10.10.0/30

HQ · 172.16.2.x / 10.10.10.4/30

Branch B · 172.16.3.x / 10.10.10.8/30

Tools & Technologies

PNetLab

Network simulation (Cisco IOL)

pfSense CE

Firewall + VPN + DHCP × 3 sites

Ansible

Infrastructure as Code automation

Wazuh XDR

SIEM — log collection & detection

Tines SOAR

No-code workflow orchestration

VirusTotal

Threat intelligence & IP reputation

Groq AI

LLM — threat analysis (Llama3)

Telegram

Real-time alert notifications

LAYER A

Infrastructure Layer — Secure Connectivity

Cisco IOL Routers

4 routers (ISP, HQ-R, BR-A, BR-B) running Cisco IOS 15.7 — authentic routing behavior without physical hardware.

pfSense Firewall × 3

Stateful inspection, default-deny rules, DHCP server, and IPsec VPN termination at every site boundary.

OSPF Dynamic Routing

FULL/DR adjacencies confirmed across all sites. Routes propagate automatically — no static route management.

IPsec Site-to-Site VPN

AES-256 encrypted tunnels between all three pfSense firewalls — all inter-site traffic is cryptographically protected.

LAYER B

Automation Layer — Infrastructure as Code

```
$ ansible-playbook site.yml
```

One command deploys the entire network across all three sites

playbook_network.yml

IP addresses + interfaces + hostnames

playbook_ospf.yml

OSPF areas + neighbor config

playbook_logging.yml

Syslog to Wazuh on all routers

playbook_wazuh.yml

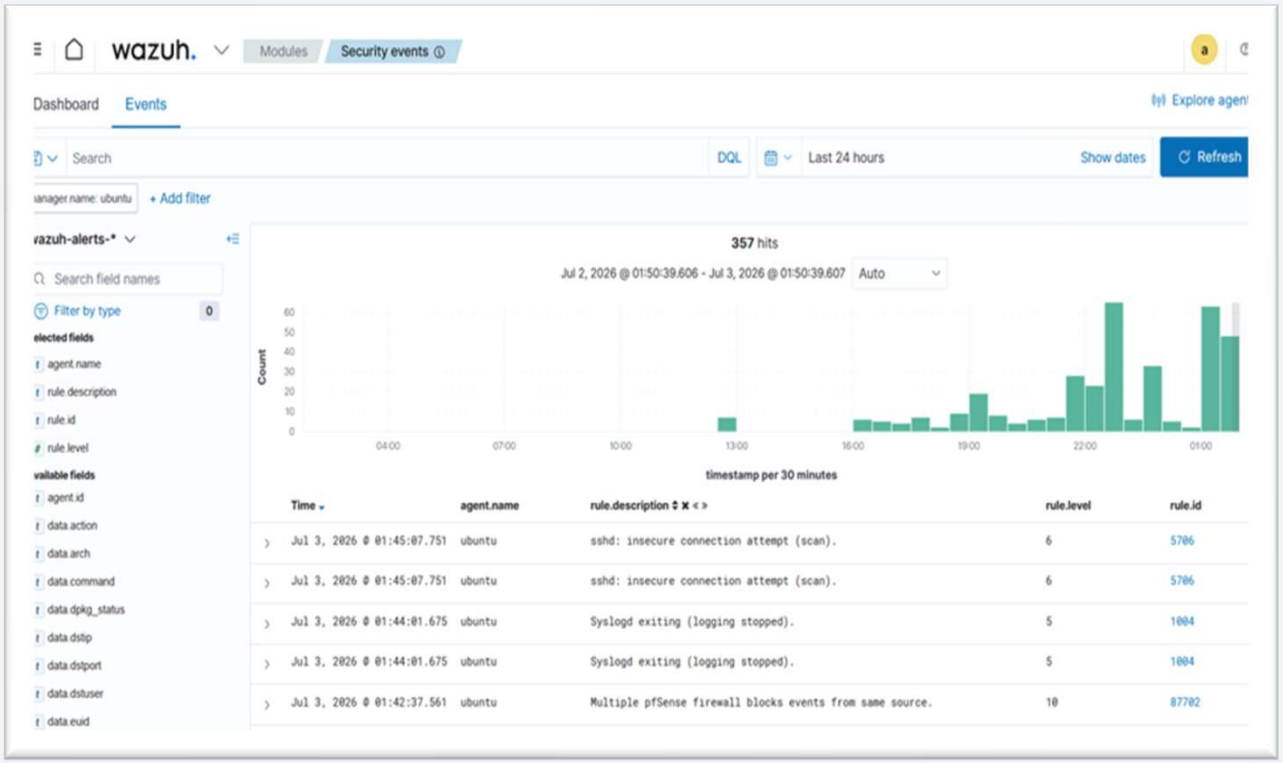
Agent install on all Linux hosts

LAYER C

Intelligence Layer — AI-Driven SOC

LAYER C

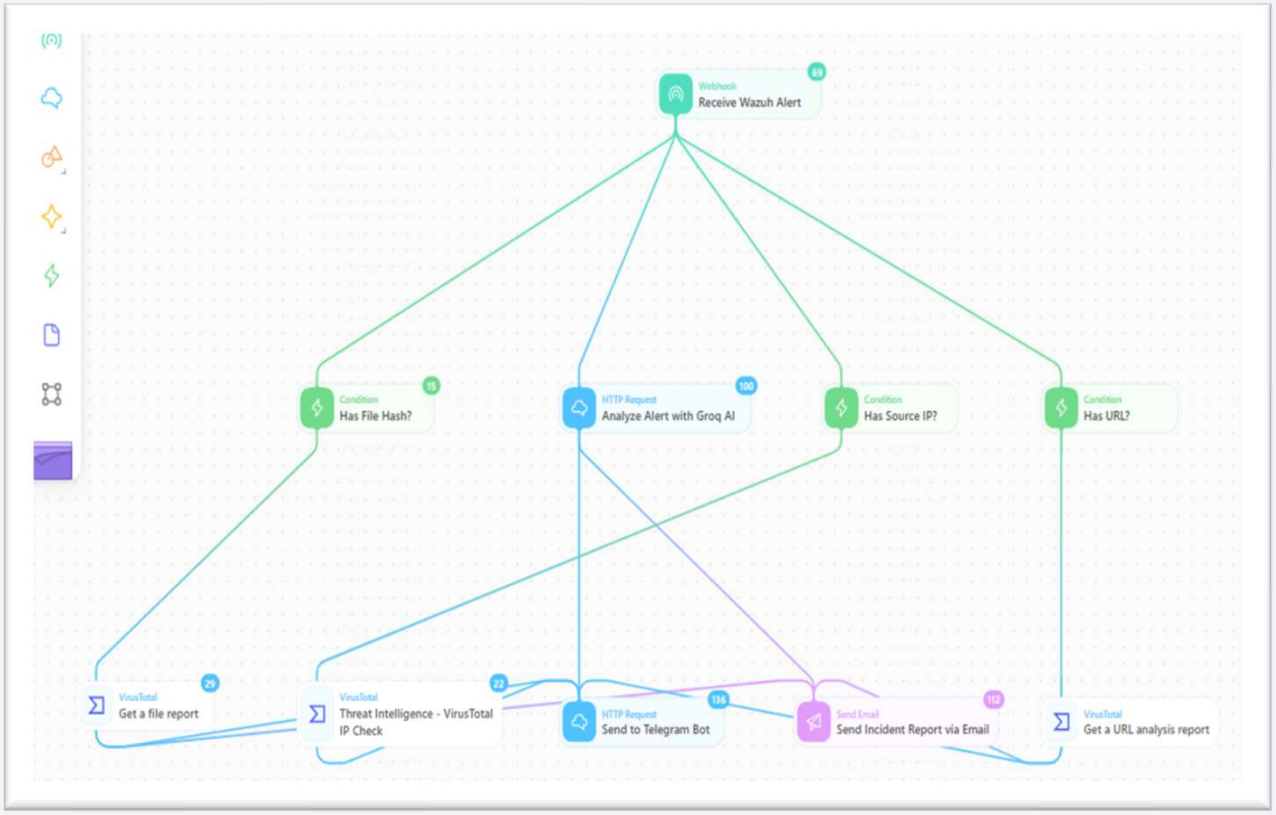
Wazuh XDR — Detection & Monitoring



- Manager-Agent architecture
- Real-time dashboard with forensic drill-down
- Active response triggers Tines webhook
- Collects syslog from all Cisco devices

LAYER C

Tines SOAR — Automated Response Workflow



1. Receives alert via Wazuh webhook
2. Queries VirusTotal for IP reputation
3. Sends enriched data to Groq AI
4. Delivers report to Telegram & Gmail

LAYER C

VirusTotal — Threat Intelligence Enrichment

```
// VirusTotal API Response
{
  "data": {
    "attributes": {
      "last_analysis_stats": {
        "malicious": 2,
        "suspicious": 0,
        "harmless": 0,
        "undetected": 69
      },
      "reputation": -6
    }
  }
```

2	-6	Potentially Malicious
Malicious Detections	Reputation Score	Verdict

LAYER C

Groq AI — Intelligent Threat Analysis

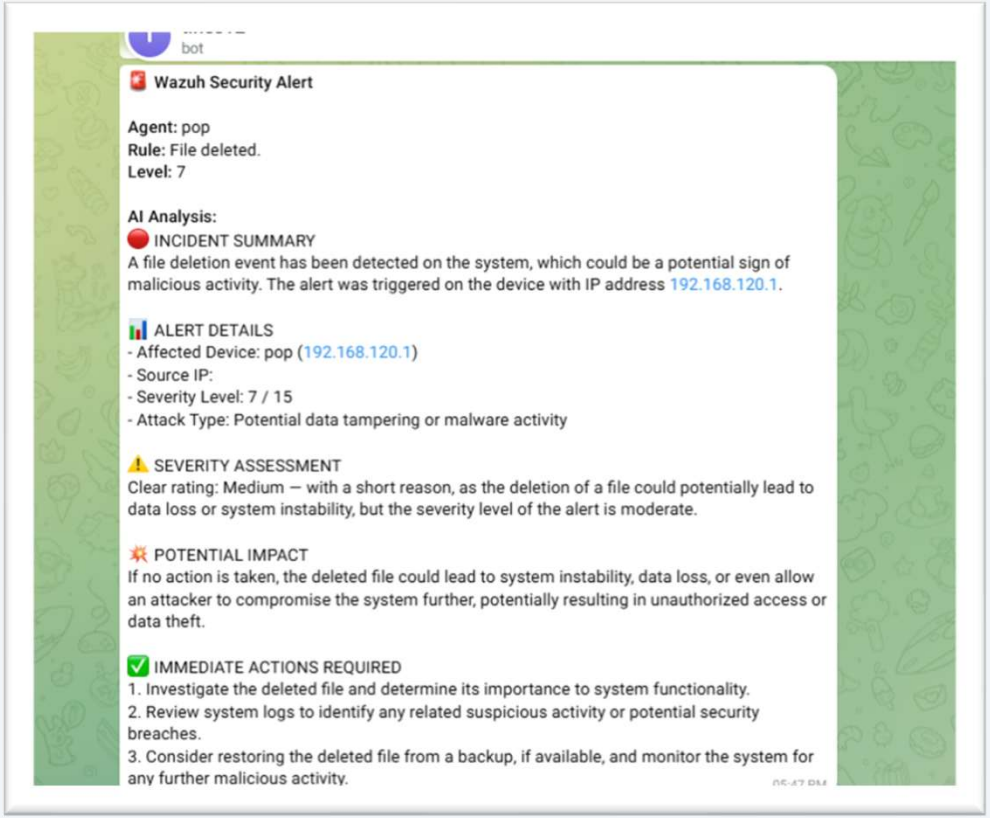

```
{
"incident_type": "File Integrity Modification",
"severity": "High",
"severity_level": 7,
"affected_host": "pop",
"affected_ip": "192.168.120.1",
"target_file": "C:\\Users\\marwa\\Downloads\\freevideo.exe",
"mitre": {
"id": "T1565.001",
"technique": "Stored Data Manipulation"
},

"analysis": "Wazuh File Integrity Monitoring detected that the monitored executable was modified.
The integrity checksum changed, indicating the file was altered after creation. The modification
should be validated to determine whether it is authorized or malicious.",

"recommended_actions": [
"Verify the file modification.",
"Compare the SHA256 hash with a trusted baseline.",
"Analyze the file using VirusTotal or a sandbox.",
```

LAYER C

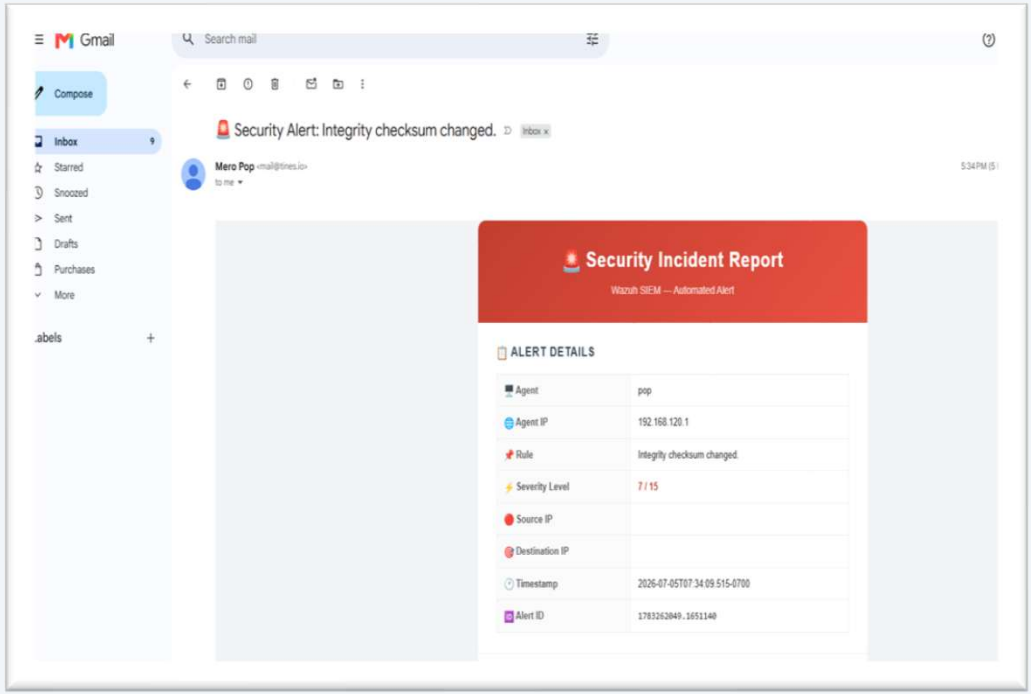
Telegram — Real-Time Alert Delivery


bot
Wazuh Security Alert
Agent: pop
Rule: File deleted.
Level: 7
AI Analysis:
INCIDENT SUMMARY
A file deletion event has been detected on the system, which could be a potential sign of malicious activity. The alert was triggered on the device with IP address 192.168.120.1.
ALERT DETAILS
- Affected Device: pop (192.168.120.1)
- Source IP:
- Severity Level: 7 / 15
- Attack Type: Potential data tampering or malware activity
SEVERITY ASSESSMENT
Clear rating: Medium — with a short reason, as the deletion of a file could potentially lead to data loss or system instability, but the severity level of the alert is moderate.
POTENTIAL IMPACT
If no action is taken, the deleted file could lead to system instability, data loss, or even allow an attacker to compromise the system further, potentially resulting in unauthorized access or data theft.
IMMEDIATE ACTIONS REQUIRED
1. Investigate the deleted file and determine its importance to system functionality.
2. Review system logs to identify any related suspicious activity or potential security breaches.
3. Consider restoring the deleted file from a backup, if available, and monitor the system for any further malicious activity.

- Delivered within seconds of attack detection
- Contains full AI-generated analysis and commands
- Accessible from any device — no VPN required
- Zero cost — Telegram Bot API is free

LAYER C

Email — Real-Time Alert Delivery



- Delivered within seconds of attack detection
- Contains full AI-generated analysis and commands
- Accessible from any device — no VPN required
- Zero cost — Telegram Bot API is free

Attack Simulation

Scenario 1 — SSH Brute Force

```
hydra -l root -P rockyou.txt ssh://10.10.20.x -t 4 -V
```

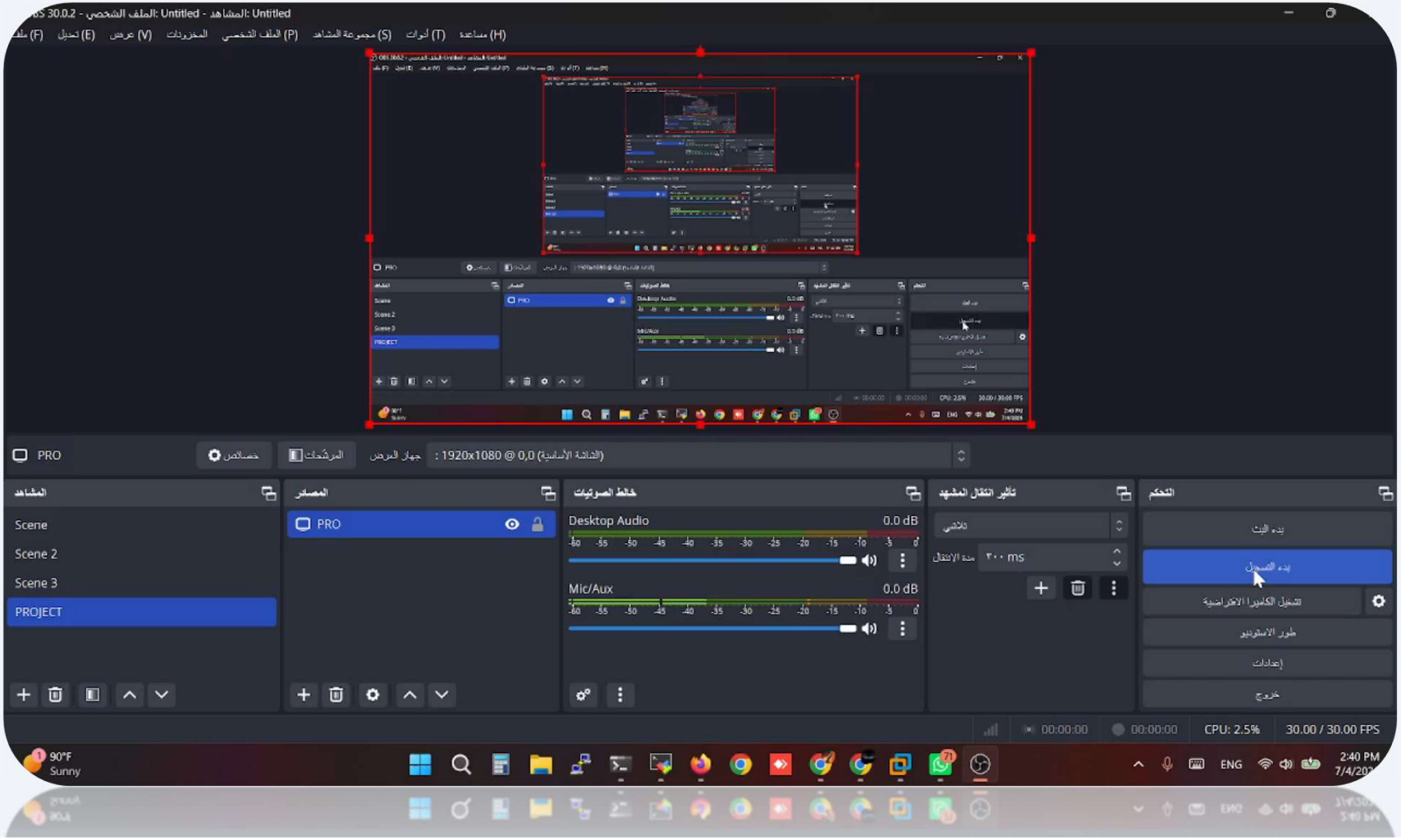
Hydra iterates a password dictionary against SSH — generates high-volume failed auth events detected by Wazuh Rule 5763.

Scenario 2 — Network Reconnaissance

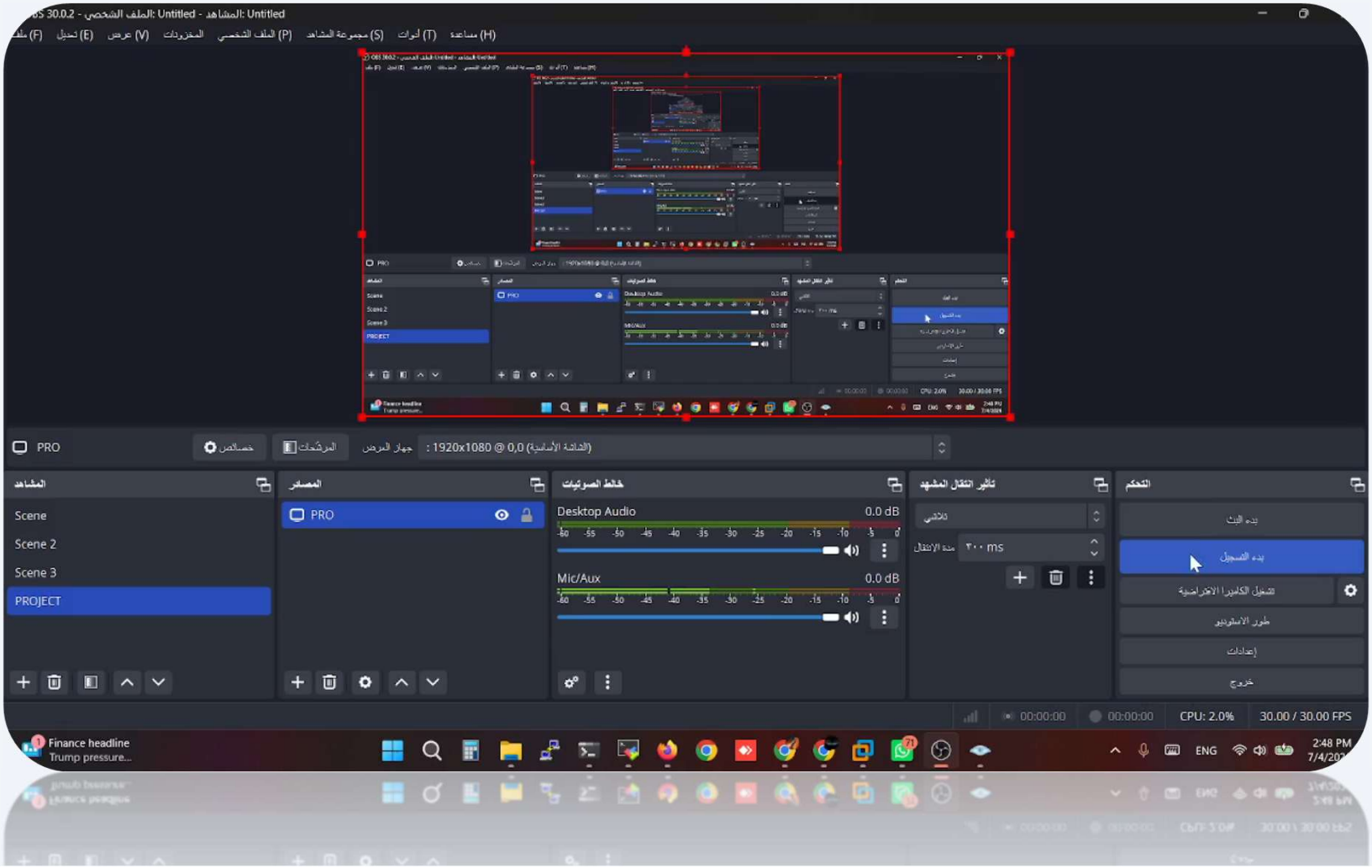
```
nmap -sV -A -T4 10.10.20.0/24
```

Aggressive port scan with service detection — triggers Wazuh reconnaissance detection rules across the HQ subnet.

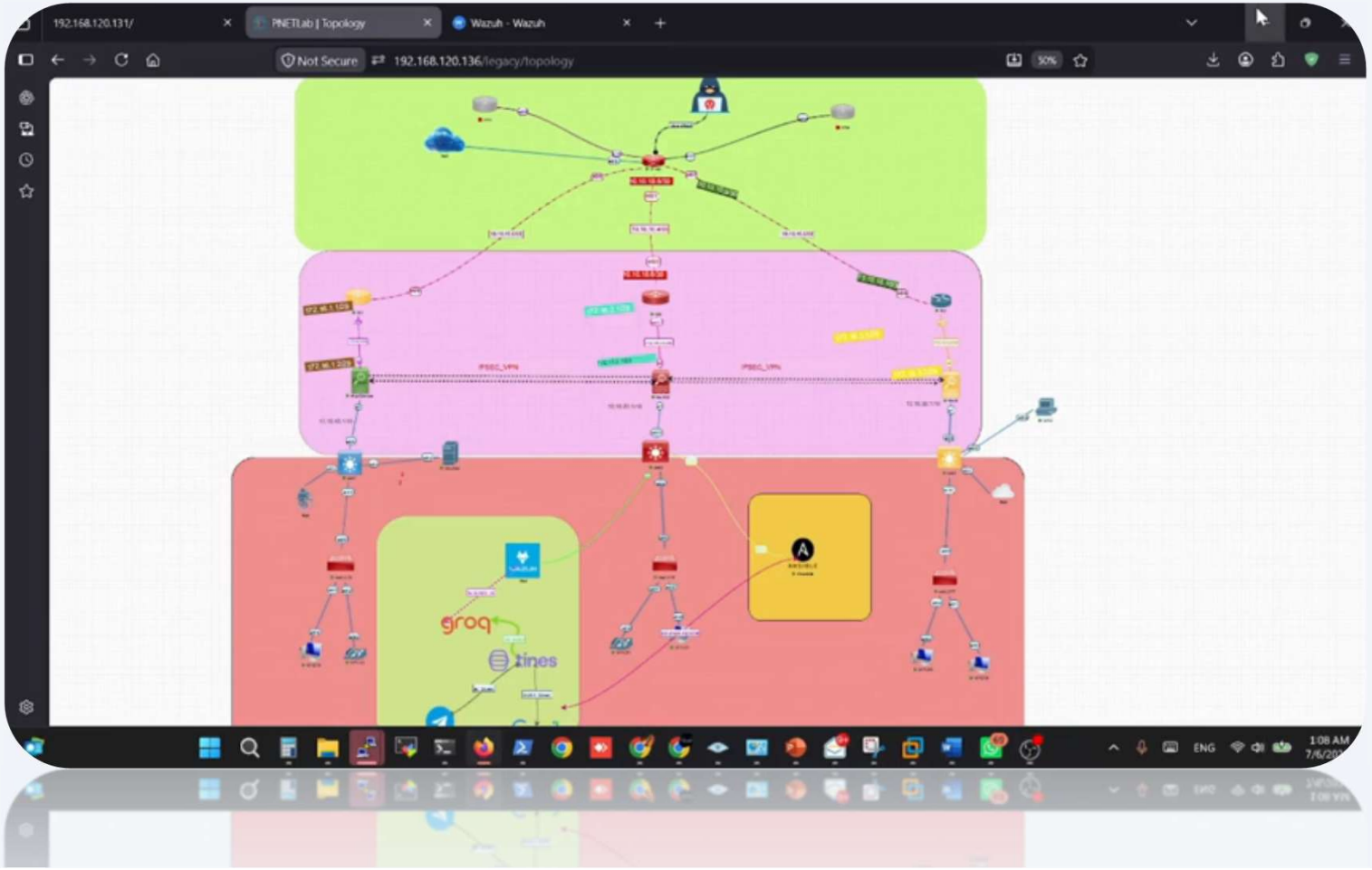
Testing Results Summary



Testing Results Summary



Testing Results Summary



Conclusion & Future Work

Achievements

- Multi-site enterprise network — fully automated
- Zero manual CLI interaction — all via Ansible
- Real-time AI threat analysis in under 3 seconds
- Complete detection-to-notification pipeline verified

Future Work

- SDN integration (OpenDaylight controller)
- Suricata IPS on pfSense for deep inspection
- Local LLM deployment (Ollama) for air-gap AI
- AWS/Azure hybrid cloud VPN extension

Thank You

Modern Hybrid Network Infrastructure · Graduation Project 2025/2026